20. The method of claim 17, wherein said second operational state is a reduced function operational state.

21. The method of claim 17, wherein said first re-boot command is operative to select one of a plurality of boot modes.

22. The method of claim 21, wherein said plurality of boot modes include a safe boot mode, a diagnostic boot mode, alternative operating system boot.

23. The method of claim 17, wherein at least one of said first and second re-boot commands are encapsulated in a network data packet according to a remote management and control protocol (RMCP) to be provided to said remote client device.

REMARKS

This response is provided to the Office Action mailed April 12, 2002. In the Office Action, claims 1-23 were declared subject to restriction and election requirement. With this response, Applicant has amended the specification to remove lingering informalities identified therein. It is noted that the amendments to the specification were not necessary to traverse the restriction requirement. Rather, the restriction requirement of claims 1-23 is traversed based, at least in part, on the remarks detailed below. In light of the foregoing amendment and subsequent remarks, reconsideration of the above-captioned application is respectfully requested.

Election

Applicant appreciates the indication that a complete response to the requirement necessarily includes an election of the invention to be examined even though the requirement be traversed. Accordingly, failing the argument(s) below, Applicant respectfully elects Group I (1-16) to be examined.

§121 Restriction Requirement of Claims 1-23

In paragraphs 1-4 of the Office Action, claims 1-23 were subject to restriction and election requirement. In particular, the Office Action suggests that such claims be divided into two disparate groups of claims 1-16 (Group I) and claims 17-23 (Group II). In response, Applicant respectfully traverses the restriction of such claims.

Applicant respectfully submits that both groups of claims are generally directed to aspects of a method and apparatus for performing network-based control functions on an alert-enabled managed client. In this regard, embodiments of Applicants' invention are generally described in accordance with the well-known client-server paradigm. Accordingly, Applicant has claims drawn to each of these various aspects of the invention.

In this regard, claim 1 recites a client that receives external control operations and conditionally executes said control operations based, at least in part, on an identified state of the client. Similarly, claim 17 is generally drawn to a server, which issues such control operations. As described herein, these control operations may include, but are not limited to, powering down, powering up, resetting and/or rebooting the client. That is, per the specification, the re-boot command is but an example of any of a plurality of suitable control commands that may be issued and selectively acted upon by a receiving client.

Group I (1-16), as designated in the Office Action, is generally directed to method(s) and apparatuses related to a client. More specifically, Group I includes claims to methods and apparatuses to receive externally provided control operations, determine the current operating state of the client, and conditionally execute the control operations if permitted in the current operating state.

Group II (17-23) includes claims directed to methods for providing control commands, of which a re-boot command is but one example control command, to the client.

Characteristically, the externally provided control operations provided to the client in Group I originate from a remote computing device (e.g., a server), while the control operation(s) claimed in Group II are intended for a remote computing device (e.g., a remote client) that may selectively perform the control operation. In this regard, despite the characterization in the Office Action, the inventive elements of the claims of proposed Group I and Group II share a common nexus and, accordingly, need not be restricted one from the other.

Accordingly, Applicant respectfully requests that the restriction requirement under 35 USC § 121 of claims 1-23 be withdrawn.

In light of the foregoing, Applicant respectfully asserts that claims 1-23, are in condition for allowance, and earnestly awaits notice thereof. **In an effort to expedite prosecution of this matter, the Examiner is invited to call the undersigned counsel for the Applicant to discuss any further issues preventing allowance of the currently pending claims.**

Please charge any shortages and credit any overages to our Deposit Account No. 02-2666.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP

Dated: May 13, 2002

Michael A. Proksch
Registration No. 43,021

12400 Wilshire Blvd.,
Seventh Floor
Los Angeles, CA 90025-1026
(503) 684-6200

Appendix A: Marked-up Version of Amended Specification to Denote Changes

(1) On page 27, please replace the paragraph from line 22 through line 4 of page 28 with:

Function_map section 620, represents functions supported on a given platform. In one embodiment, as indicated by reference number [622] **621**, the data in the function map appears as ordered pairs of integers. In one embodiment, the first integer is a generic external representation of the function as provided in the function_list section (described above), and the second integer is an internal representation of the event that may differ depending upon the particular platform involved.

(2) On page 30, please replace the paragraph from line 14 through line 5 of page 31 with:

Like the RMCP header section, RMCP data section 830 also contains various fields including: event code field 832, data length field 834, checksum field 836, and data field 839. Event code field 832 contains data that indicates the type of event that has occurred on the client as explained above with respect to Figures 4A, 4B and 5. If event code field 832 indicates that a "simple" event "1" has occurred, the alert proxy references the Event_map section of its description file to determine an appropriate direct event mapping. Data length field 834 is used to indicate the length of the RMCP data section that follows. In one embodiment, data length field 834 is assigned a fixed value representing a length of 46 bytes. Checksum field 836 appears in both the RMCP transmit packet format and receive packet format, but is [used] implemented differently in each. In the RMCP transmit data packet, the UDP checksum is used by the system rather than an RMCP-specific checksum that utilizes checksum field 836. In transmit mode therefore, the value of checksum field 836 is set equal to zero since the field remains unused. Data field 839 may contain data that provides additional event descriptions to be parsed and used by the alert proxy.